



Office of the Inspector General
United States Department of Justice

Statement of Glenn A. Fine
Inspector General, U.S. Department of Justice

before the

House Committee on Appropriations
Subcommittee on Science, the Departments of State,
Justice, and Commerce, and Related Agencies

concerning

The Federal Bureau of Investigation

September 14, 2005

**Statement of Glenn A. Fine
Inspector General, U.S. Department of Justice,
before the
House Committee on Appropriations
Subcommittee on Science, the Departments of State, Justice, and
Commerce, and Related Agencies
concerning
The Federal Bureau of Investigation
September 14, 2005**

Mr. Chairman, Congressman Mollohan, and Members of the Subcommittee on Appropriations:

Thank you for inviting me to testify about the Office of the Inspector General's (OIG) oversight work regarding the Federal Bureau of Investigation (FBI). After the September 11, 2001, terrorist attacks, counterterrorism became the top priority of the FBI and of the Department of Justice. The FBI is undergoing an extensive transformation, driven by its new priorities, that reallocates its investigative resources from traditional crime areas to terrorism-related matters. As a result, much of the OIG's work in the past 4 years has examined FBI programs and operations related to counterterrorism and national security issues, as it undergoes this significant transformation.

These OIG reviews include reports on the FBI's information technology initiatives such as the Trilogy Project and the Virtual Case File effort; the FBI's foreign language translation program; the FBI's compliance with the Attorney General Guidelines governing the use of confidential informants and other investigative techniques; the recruitment and training of FBI intelligence analysts; the FBI's management of the Terrorist Screening Center; intelligence information in the FBI's possession prior to the September 11 attacks; and the FBI's participation in various Department counterterrorism task forces.

In addition, the OIG currently is examining other FBI programs and operations, including its progress in developing the Sentinel information technology program, the impact on other federal and state law enforcement organizations as a result of the changes in the FBI's allocation of investigative resources, issues surrounding the FBI's observations of alleged mistreatment of detainees at Guantanamo and other military detention facilities, a follow-up review of the FBI's changes in its internal security procedures as a result of the Hanssen case, and the FBI's handling of the Brandon Mayfield matter.

In this written statement, I provide a description of these ongoing OIG reviews, as well as a summary of the findings of several of the completed OIG reviews.

However, at the outset of this statement, I want to offer several observations about the FBI and the key challenges it faces as it continues its transformation. These observations are based on numerous OIG reviews, as well as my more than 10 years in the OIG interacting with the FBI, the last 5 years as Inspector General.

It is clear that the FBI is undergoing significant transformation on multiple fronts simultaneously, a difficult task in any large organization. The FBI's transformation will not happen immediately or easily. A variety of OIG reviews, many of which I summarize in this statement, have identified shortcomings in the FBI's efforts to remake itself and have highlighted areas in need of greater progress. However, despite the deficiencies we have found, I believe that Director Mueller is a strong leader who is moving the FBI in the right direction. Moreover, we have found the FBI generally receptive to the recommendations in OIG reports and it usually has agreed with the need to implement most of them.

I also want to note that while the OIG has described problems in a number of important FBI programs over the years, this should in no way diminish the contributions that dedicated FBI employees make on a daily basis. Many FBI employees throughout the country and the world perform their jobs diligently, often under very difficult circumstances, and their work is essential to the safety and security of the country.

However, there are several areas that I believe need significant improvement. The first is the urgent need to upgrade the FBI's information technology systems. In essence, the FBI is in the business of uncovering, analyzing, sharing, and acting on information. To do so effectively, it must have adequate information technology and case management systems. But the FBI's current information technology systems are far short of what is needed. As we have reported in several reviews, the FBI's efforts to create a modern case management system to catalogue, retrieve, and share case information throughout the agency have still not succeeded. Past OIG reports have described the problems the FBI's inadequate systems have created, such as our report describing the belated production of documents in the McVeigh case and the report on the FBI's handling of intelligence information related to the September 11 attacks. I believe that the upgrade of the FBI's information technology systems is one of the most critical challenges facing the FBI. Without adequate systems, the FBI will not be able to perform its job as effectively and fully as it should. As a result, as I describe later in this statement, the OIG has monitored, and will continue to review, the FBI's

important FBI information technology initiatives, including the Sentinel project. I know this Subcommittee has taken an important role in overseeing the FBI's information technology projects, and has asked that we continue to review the FBI's IT initiatives.

Second, the FBI faces many challenges in the human capital area. I believe that some of the problems we found in our various reviews stem from high turnover in important positions throughout the FBI. We often see FBI employees in leadership positions for short periods of time. For example, turnover in key positions hurt the FBI's ability to manage and oversee the Trilogy information technology modernization project. Between November 2001 and February 2005, 15 different key information technology managers were involved with the Trilogy project, including 5 FBI Chief Information Officers and 10 individuals serving as project managers for various aspects of Trilogy. This lack of continuity contributed to the ineffective and untimely implementation of the Trilogy project. Similarly, the FBI's counterterrorism division has had five leaders in the last 4 years. We also have seen rapid turnover in FBI field office managers. While some turnover is healthy in any organization, the rapid change in important positions throughout the FBI is unduly high, and I believe this turnover hurts the FBI's ability to transform itself and fulfill its mission.

A third critical challenge facing the FBI is its need to share intelligence and law enforcement information efficiently, both within the FBI and with its law enforcement and intelligence partners. The FBI has made progress over the past several years in this area. For example, the OIG's review of Joint Terrorism Task Forces found that the FBI has made strides in sharing information with state and local partners, who are critical to the nation's counterterrorism efforts. But more must be done, particularly with regard to sharing intelligence information with other federal agencies. The FBI is only part of the nation's counterterrorism and counterintelligence efforts, and it must share its information effectively with other agencies.

Fourth, I believe the FBI must value and support to a greater degree FBI staff with technical skills. For example, until recently, the FBI did not adequately value the contributions of intelligence analysts. The FBI's general view was that special agents performed the key work of the agency, and intelligence analysts were used primarily to support ongoing cases. Special agents historically were promoted to technical leadership positions within the FBI, such as handling information technology upgrades or leading scientific efforts in the laboratory. While this culture is changing, more needs to be done to support the work of intelligence analysts, scientists, linguists, and other staff who are critical to meeting the FBI's changing mission and duties.

Fifth, the FBI and Director Mueller should receive credit for opening the FBI to outside scrutiny much more than in the past. The FBI previously had

an insular attitude, with an aversion to outside scrutiny or oversight. For example, until 2001 allegations of misconduct against FBI employees were not subject to outside review by the OIG, but were handled in-house by the FBI.

I believe the FBI's attitude is changing. As described below, the OIG now has jurisdiction to investigate misconduct in the FBI, and we have received good cooperation from the FBI in this new role. The FBI also has opened its programs and management to outside scrutiny from groups such as the National Academy of Public Administration, the Government Accountability Office, and other oversight entities. In addition, the FBI now is more willing to seek outside advice and support.

Not everyone in the FBI has welcomed such change and outside scrutiny with open arms. But I believe that senior FBI leadership and most FBI employees recognize the need for such change and see the benefit of outside oversight. Director Mueller deserves credit for promoting this change in attitude throughout the FBI, even though the transformation is not yet complete.

Based on the many reviews of the FBI conducted by the OIG, I believe the FBI faces significant challenges and needs to make greater progress in many important areas. In this statement, I discuss several OIG reviews that provide a window on the challenges confronting the FBI, where it has made progress, and where additional improvement is needed.

My statement is organized in three main parts. In the first section, I provide background information on the OIG's oversight responsibilities in the FBI and how these responsibilities have changed over the past several years. Second, I summarize the results of a review issued by the OIG this week that examined the FBI's implementation of four sets of guidelines issued by the Attorney General in May 2002: the Attorney General's Guidelines Regarding the Use of Confidential Informants; Guidelines on FBI Undercover Operations; Guidelines on General Crimes, Racketeering Enterprise, and Terrorism Enterprise Investigations; and the Revised Department of Justice Procedures for Lawful, Warrantless Monitoring of Verbal Communications. Third, I briefly summarize a series of ongoing reviews in the FBI and the results from several recently completed OIG reviews of FBI programs.

I. INSPECTOR GENERAL OVERSIGHT OF THE FBI

The OIG accomplishes its oversight responsibilities in the FBI through audits, inspections, investigations, and special reviews. The OIG's Investigations Division investigates allegations of criminal and administrative misconduct throughout the entire Department of Justice, including in the FBI. The OIG's Audit Division conducts audits of FBI programs and activities,

including audits of the FBI's annual financial statements and computer security audits of FBI information technology systems. The OIG's Evaluation and Inspections Division conducts program reviews to assess the effectiveness of FBI operations. The OIG's Oversight and Review Division uses attorneys, investigators, and program analysts to conduct systemic reviews involving FBI programs or allegations of misconduct involving senior FBI officials, such as the review of the FBI's performance in the Hanssen case.

Since its creation in 1989, the OIG has had the authority to conduct audits and inspections throughout all DOJ components. However, until July 2001, the OIG did not have jurisdiction to investigate allegations of misconduct in the FBI or the Drug Enforcement Administration (DEA) and therefore the FBI and DEA conducted their own investigations of employee misconduct. On July 11, 2001, the Attorney General expanded the OIG's authority to investigate allegations of misconduct in the FBI and the DEA. In November 2002, Congress codified the OIG's authority to investigate allegations of misconduct involving FBI and DEA employees.¹

Similar to our practices with other DOJ components, the OIG now reviews all allegations of misconduct against FBI employees and investigates the most serious ones, including allegations that if proved would result in prosecution and serious allegations against high-level FBI employees. We normally refer other allegations back to the FBI for it to handle, as we do with other DOJ components.

While the FBI initially was not enthusiastic about the OIG's expanded jurisdiction to investigate misconduct allegations against its employees, I am pleased to report that it has cooperated well with OIG investigations, both at FBI headquarters and in the field.

II. OIG REVIEW OF THE FBI'S COMPLIANCE WITH REVISED ATTORNEY GENERAL INVESTIGATIVE GUIDELINES

Earlier this week, the OIG issued a review that examined the FBI's compliance with four sets of Attorney General Guidelines that govern the FBI's principal criminal investigative authorities with respect to investigations of individuals and groups, and its use of confidential informants, its undercover operations, and its warrantless monitoring of verbal communications (also known as consensual monitoring). Since the mid-1970s, the Attorney General Guidelines have defined the circumstances that justify opening of an FBI

¹ There is only one exception to the OIG's investigative jurisdiction throughout the Department. The OIG does not have authority to investigate allegations of misconduct involving DOJ attorneys acting in their capacity to litigate, investigate, or provide legal advice or investigators working under the direction of DOJ attorneys. That responsibility is given to the Department's Office of Professional Responsibility (DOJ OPR).

investigation, the permissible scope of an investigation, and the law enforcement techniques the FBI may use.

Following the September 11, 2001, terrorist attacks, the Attorney General ordered a comprehensive review of the Attorney General's Guidelines to identify revisions that would enhance the Department's ability to detect and prevent such attacks. On May 30, 2002, the Attorney General issued revised Investigative Guidelines that provided FBI field managers with greater authority to conduct preliminary inquiries, criminal intelligence investigations, and undercover operations.

To conduct this review, the OIG examined nearly 400 investigative files in 12 FBI field offices throughout the country, interviewed FBI and DOJ personnel, reviewed thousands of FBI documents, and surveyed FBI field personnel and federal prosecutors throughout the country.

In sum, while the OIG found many areas in which the FBI complied with the Attorney General Guidelines, the OIG found significant non-compliance with the Guidelines governing the operation of confidential informants, failure to notify FBI Headquarters and DOJ officials of the initiation of certain criminal intelligence investigations, and failure to consistently obtain advance approval prior to the initiation of consensual monitoring. The OIG also identified serious shortcomings in training on the Guidelines and the FBI's planning for and implementation of the revised Guidelines. Among the specific findings in the OIG's report:

- The OIG review found one or more Guidelines violations in 87 percent of the confidential informant files we examined. These errors occurred in several of the most important aspects of the FBI's management of the Criminal Informant Program: initial and continuing suitability reviews designed to assess the suitability of individuals to serve or continue as confidential informants (non-compliance found in 34 percent and 77 percent of the files, respectively); the instructions FBI agents are required to give confidential informants (49 percent non-compliant files); the FBI's use of its power to authorize confidential informants to participate in "otherwise illegal activity" (60 percent non-compliant files); the notification requirements associated with a confidential informant's commission of "unauthorized illegal activity" (42 percent non-compliant files); and the documentation and notice requirements triggered when a confidential informant is deactivated (37 percent non-compliant files).

The OIG focused on these aspects of the FBI's informant program because they include many of the critical judgments the FBI must make to ensure that individuals registered as confidential informants are suitable, that they understand the limits of their authority from the FBI,

and that supervisory DOJ officials approve or are notified of significant developments regarding the confidential informants. The OIG review determined that required approvals were not always obtained, suitability assessments were not made or were incomplete, documentation of required instructions were missing, descriptions of “otherwise illegal activity” were not sufficient, and notifications to FBI Headquarters or U.S. Attorneys’ Offices were not made or documented.

While confidential informants are critical to the successful prosecution of individuals and criminal enterprises, the OIG report explains that handling confidential informants presents serious risks, including the risk that informants may claim that their criminal activities were authorized or acquiesced in by the government. Consequently, Guidelines violations can jeopardize DOJ prosecutions of criminals and can also lead to civil liability claims against the government.

- FBI Headquarters has not sufficiently supported the FBI’s Criminal Informant Program, which in turn has hindered FBI agents in complying with the Confidential Informant Guidelines. In many instances, agents lacked access to basic administrative resources and guidance that would have promoted compliance with the Confidential Informant Guidelines. Among the shortcomings identified in the report were the failure to provide standardized forms to record suitability assessments, supervisory approvals, instructions to informants, and procedures triggered by the deactivation of informants; a field guide to assist agents in complying with the Guidelines; and other administrative and technological support.
- Compliance with the Confidential Informant Guidelines varied significantly by FBI field office. In some offices, the FBI’s failure to follow well-established DOJ and FBI regulations governing the use of confidential informants was widespread and persistent over many years, and resulted from serious problems with supervisory oversight and agent accountability. In contrast, the OIG identified other FBI field offices from FBI inspection reports with consistently good compliance records that the OIG attributed to highly motivated and experienced personnel and effective field-level management.
- The OIG review found, in contrast to the FBI’s compliance with the Confidential Informant Guidelines, the FBI generally was compliant with the Undercover Guidelines, and the Headquarters unit supporting undercover operations was well managed and effective. For example, this unit had generated an up-to-date field guide and standardized forms, and used technology such as a centralized database that assists in effectively monitoring undercover operations.

- The FBI also generally adhered to the provisions of the General Crimes Guidelines. However, the FBI has not developed adequate controls to ensure that required notifications of the initiation and renewal of criminal intelligence investigations are made to U.S. Attorneys and DOJ on a timely basis and documented in the case files, that authorizations for the extension and renewal of preliminary inquiries and for the conversion of preliminary inquiries to full investigations are documented, that FBI Special Agent in Charge reviews of criminal intelligence investigations are documented, and that progress reports to DOJ on certain terrorism enterprise investigations are included in the case files.
- Part VI of the General Crimes Guidelines grants the FBI new authorities to visit public places and attend public events to detect or prevent terrorist activities in the absence of particularized evidence that a crime has occurred or is likely to occur. The OIG found that the FBI encourages but does not require agents to obtain supervisory approval prior to using these authorities to visit public places or attend public events. Moreover, neither FBI field offices nor FBI Headquarters consistently maintains records regarding the use of and compliance with these authorities, including the provisions that address the FBI's authority to collect, maintain, and disseminate information obtained at such events and provisions forbidding retention of certain information. Because of the lack of documentation regarding approval of such visits, or documentation regarding the visits, the OIG was unable to draw conclusions about the FBI's utilization of these authorities or its compliance record.
- The FBI generally was in compliance with the Consensual Monitoring Guidelines, although the OIG identified several deficiencies, particularly with regard to the Guidelines' requirements for supervisory authorization of the consensual monitoring. In approximately nine percent of the monitorings reviewed, the OIG found that the authorization post-dated the first recording.

The OIG also examined the operation of various FBI and DOJ mechanisms designed to promote compliance with the Guidelines. The review found that two joint FBI-DOJ committees that approve or oversee confidential informants and undercover operations are operating effectively and contribute to Guidelines compliance. By contrast, the OIG review found that key FBI field personnel with special expertise and responsibility for Guidelines compliance (such as Informant Coordinators, Undercover Coordinators, and Division Counsel) were not uniformly consulted regarding investigative activities and sometimes were not adequately supported in their efforts to promote compliance with the Guidelines and internal FBI policy.

In the report, the OIG offers 47 recommendations designed to promote greater accountability for Guidelines violations by field supervisors; to use existing technology to track Guidelines violations; to enhance training on Guidelines requirements and the consequences of Guidelines violations to FBI investigations and DOJ prosecutions; to require supervisory approval and more systematic recordkeeping on the FBI's use of new authorities to visit public places and attend public events for the purpose of detecting and preventing terrorist activities; and to prepare a comprehensive implementation strategy for the next Guidelines revisions. The FBI concurred with 43 of the 47 recommendations, and concurred partially with the 4 remaining recommendations.

III. ADDITIONAL OIG REVIEWS OF FBI PROGRAMS

A. Ongoing OIG Reviews in the FBI

The OIG currently is conducting a series of reviews of a variety of important FBI programs. The following are examples of ongoing OIG reviews:

Oversight of the FBI's Sentinel Case Management Project: In March 2005, the FBI announced plans to develop the Sentinel Case Management system to replace the failed Virtual Case File effort. The FBI stated that it hoped to use modular off-the-shelf components for Sentinel and expected to implement the new case management system in a phased approach over 39 to 48 months. On August 8, 2005, the FBI issued a "Request for Proposals" to develop the new system. The FBI stated that it plans to award the contract in November 2005 and begin development work in early 2006.

At the request of the FBI Director and this Subcommittee, the OIG intends to closely monitor the FBI's implementation of its Sentinel project. Several months ago we began an audit of the Sentinel project. Initially, this audit is focusing on the FBI's planning for the project, including the FBI's approach to developing the system, management controls over the project, information technology management processes, project baselines, contracting processes, and funding sources. Rather than issue a single audit report, we anticipate completing a series of audits about discrete aspects of the Sentinel project, such as the FBI's monitoring of the contractor's performance against established baselines and the progress of the project.

To date, the FBI has been responsive in meeting our requests for information and access to personnel (with the exception of providing complete system cost estimates due to the procurement-sensitive nature of that information). After analyzing the information obtained from FBI documents and the results of our interviews with key FBI personnel, including the FBI's

Chief Information Officer (CIO), we believe that the FBI has instituted important information technology investment management processes and management controls that it did not have when it attempted to complete the Virtual Case File. While it is too early to state with confidence that the Sentinel project will be successful, we do have some preliminary observations about the FBI's handling of Sentinel and how its oversight of this project has changed since the Virtual Case File effort.

The OIG's February 2005 audit of Trilogy and the Virtual Case File identified a number of reasons why the Virtual Case File VCF portion of Trilogy failed, including poorly defined and slowly evolving design requirements, IT Investment Management weaknesses, lack of an Enterprise Architecture, and lack of management continuity and oversight. Our preliminary review of Sentinel indicates that, for the most part, the FBI is attempting to address these weaknesses in preparing for the Sentinel project. Specifically, the FBI has taken the following actions:

Design Requirements and IT Investment Management Processes: Unlike the Virtual Case File, the FBI has identified, and intends to freeze, the Sentinel requirements. Any significant changes to the specifications must be approved by the FBI's Deputy Director. Sentinel's system requirements have undergone two reviews, or Control Gates, by internal boards representative of various units in the FBI, which reviewed and approved the system requirements. Further, an Independent Verification and Validation process will test the system as it is developed, monitoring the contractor as well as the FBI's management of the project.

Enterprise Architecture: The FBI continues to refine its Enterprise Architecture. An Enterprise Architecture is a strategic information plan that defines an organization's mission, the information and technologies necessary to perform that mission, and the transitional processes for implementing new technologies in response to changing mission needs. In essence, the Enterprise Architecture provides frames of reference that allow an understanding of what an enterprise does; when, where, how, and why it does it; and what it uses to accomplish its mission. The FBI expects Sentinel to align with its Enterprise Architecture.

Management Continuity: The Trilogy project, including the Virtual Case File, was plagued with turnover of FBI CIO and Program Managers and a lack of program expertise. Since then, the FBI has consolidated IT functions and management under one CIO, has "borrowed" an experienced Program Manager from another agency to manage Sentinel, and is in the process of attempting to build a professional program management staff to help ensure that the Sentinel project stays on track and within budget.

Oversight: The FBI is relying on more oversight and advice for Sentinel. Among the groups advising the FBI and helping to monitor the Sentinel project are the FBI's Science and Technology Board, RAND, the Markle Foundation, and other consultants and contractors such as Aerospace Corporation.

However, despite these apparent improvements, our preliminary work has identified several issues of concern that the FBI will need to focus on in order to successfully develop and deploy the Sentinel case management project. For example, the FBI's Sentinel Program Management Office is not yet fully organized and staffed with systems engineers, contracting officers, and budget personnel. Further, the Sentinel Program Manager, on loan from another agency, has committed to 2 years with an option for a third year. Given the anticipated time frame for developing this project, the Program Manager may have to be replaced before Sentinel is completed and deployed. As noted above, turnover of key personnel during the Trilogy effort undermined that project.

The FBI has established seven "control gate reviews" for its information technology projects and, since July 2005, Sentinel has undergone two control gate reviews. The first gate was a System Concept Review, which approved the recommended system Concept of Operations. The second gate was an Acquisition Plan Review, which approved the Systems Specification and Interface Control documents and the approach and resources needed to acquire the system. However, these two reviews identified a number of risks, which the OIG will review and monitor throughout our audits. These risks include:

- The program award schedule is very aggressive.
- Sentinel phases must interface with numerous legacy systems operated outside the FBI's Office of the CIO.
- Parallel FBI initiatives could result in scope creep for the Sentinel project.
- FBI mission or user requirements could change and also result in scope creep.
- Evolving Enterprise Architecture standards could present new design problems
- Initial project costs are underestimated.

We also note that the FBI is the lead agency for developing an interagency Federal Investigative Case Management System framework with Sentinel serving as the application of that framework for eventual adoption by other federal agencies. The Department of Homeland Security and other participating agencies are relying on the successful development of Sentinel to

meet their own case management needs and enhance information sharing within the federal law enforcement community. However, the FBI did not incorporate input from these other agencies on the design for Sentinel, including its information sharing requirements. As was learned from our review of the FBI's Virtual Case File effort, one key to successful information technology projects is well-defined requirements that do not significantly change while the system is being developed.

Finally, the FBI plans to fund the Sentinel project in four phases, some of which may overlap. We understand that the FBI intends to reprogram funds to pay for the first two phases of the Sentinel project. As part of our ongoing audit, we plan to examine the amount of funding required, the source of funding to bring the multi-phase project to completion, and the effect of significant reprogramming on other critical FBI operations such as counterterrorism.

FBI Observations of and Reports Regarding Detainee Treatment at Guantanamo Bay and other Military Facilities: The OIG currently is examining FBI employees' observations and actions regarding alleged abuse of detainees at Guantanamo Bay, Abu Ghraib, Afghanistan, and other venues controlled by the U.S. military. The OIG is investigating whether FBI employees participated in any incident of detainee abuse in military facilities at these locations, whether FBI employees witnessed incidents of abuse, how FBI employees reported observations of alleged abuse, and how those reports were handled by the FBI.

As part of this ongoing review, the OIG has interviewed detainees, FBI employees, and military personnel at Guantanamo. In addition, the OIG has administered a detailed questionnaire to approximately 1,000 FBI employees who served assignments at military detention facilities. The questionnaire requested information on what the FBI employees observed, whether they reported observations of concern, and how those reports were handled. The OIG has received over 900 responses to its questionnaire, and the investigative team is also conducting appropriate follow-up interviews.

It is important to note that the actions of military personnel are not within the jurisdiction of the DOJ OIG and therefore are not the subject of the OIG's review. Rather, those actions are the subject of reviews by Department of Defense officials. However, the OIG is coordinating its work with a military review conducted by the U.S. Southern Command, which reviewed instances of alleged mistreatment of detainees at Guantanamo Bay that are cited in FBI documents.

Effects of the FBI's Reprioritization: The OIG is completing another review of the changes in the FBI's allocation of its personnel resources since

the September 11 terrorist attacks. This is the third in a series of reviews examining the changes in the FBI's allocation of investigative resources since the September 11 attacks. This review is assessing how the FBI's reprioritization efforts and the shift of resources from more traditional criminal investigative areas, such as drugs and white collar crime, to terrorism has affected other federal, state, and local law enforcement organizations.

In this review, we analyzed FBI data and documentation from FYs 2000 through 2004 to identify the specific changes in the FBI's investigative efforts related to traditional crime areas. We also examined case management data from the Executive Office for United States Attorneys, which showed changes in the number of criminal matters that the FBI had referred to United States Attorneys' Offices. In addition, we interviewed Headquarters and field officials at the FBI and other federal law enforcement entities, such as the Drug Enforcement Administration (DEA), the Executive Office of the President's High Intensity Drug Trafficking Area Program, and the United States Marshals Service, to determine the impact of the FBI's changed investigative priorities. Further, to obtain the views of state and local law enforcement officials, we disseminated a web-based survey to approximately 3,500 state and local law enforcement agencies. We also conducted interviews with field-level state and local officials.

Our review will describe in detail the overall changes in the FBI's criminal investigative efforts, including the changes in FBI positions allocated for criminal investigations as well the changes in actual usage of criminal agents. We also focus on the changes in specific criminal investigative areas, such as drug trafficking, financial crimes, organized crime, gang investigations, fugitive apprehensions, bank robberies, public corruption, and other criminal areas. In examining these changes, we also attempt to assess the impact of the FBI's changed focus on other federal, state, and local law enforcement agencies.

FBI's Handling of the Brandon Mayfield Matter: The OIG is finishing its investigation of the FBI's conduct in connection with the erroneous identification of a fingerprint found on evidence from the March 2004 Madrid train bombing. The FBI's fingerprint examiners erroneously concluded that the fingerprint belonged to Brandon Mayfield, an attorney in Portland, Oregon. As a result of the misidentification, the FBI initiated an investigation of Mayfield that resulted in his arrest as a "material witness" and his detention for approximately two weeks. Mayfield was released when Spanish National Police matched the fingerprints on the evidence to an Algerian national. The OIG is examining the cause of the erroneous fingerprint identification and the FBI's handling of the matter, including the investigation of Mayfield. The Department of Justice Office of Professional Responsibility is reviewing the conduct of the prosecutors in the case.

In our review, the OIG has consulted with national fingerprint experts to assist in the evaluation of the causes for the fingerprint misidentification. The OIG report also will examine the corrective actions taken by the FBI Laboratory since the misidentification came to light. In addition, the OIG report will address issues arising from the FBI's investigation and arrest of Brandon Mayfield, including any use of or implication of the Patriot Act in this case, the FBI's participation in the preparation of the material witness and criminal search warrants, and Mayfield's conditions of confinement while he was held as a material witness. The OIG is nearing the completion of its review, and we are currently drafting our report of investigation.

Follow-Up Review Regarding OIG Report on Espionage of Robert Hanssen: The OIG recently initiated a review of the FBI's progress in implementing the recommendations contained in the OIG's August 2003 report entitled, "A Review of the FBI's Performance in Deterring, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen." Hanssen's espionage began in November 1979 – 3 years after he joined the FBI as a special agent – and continued intermittently for more than 20 years until his arrest in February 2001. The OIG concluded that Hanssen escaped detection for so long not because he was extraordinarily clever and crafty, but because of long-standing systemic problems in the FBI's counterintelligence program and a deeply flawed internal security program. The OIG's report made 21 recommendations to help the FBI improve its internal security program and enhance its ability to deter and detect espionage.

The Hanssen follow-up review will assess the FBI's progress in addressing the report's recommendations. Those recommendations relate to five general areas: (1) improving the FBI's performance in detecting FBI penetration; (2) improving coordination with the Justice Department; (3) improving source recruitment, security, and handling; (4) security improvements; and (5) management and administrative improvements. In conducting the review, we plan to review FBI policy statements, manuals, and other documents that address the FBI's corrective actions, and interview relevant FBI and DOJ personnel to determine the status of the FBI's actions.

Seaport Security: The OIG recently began a review of the FBI's role in helping to secure the nation's 361 seaports. The United States has the world's most extensive and complex port system. Many ports are adjacent to major population centers, transportation hubs, and industrial facilities where petroleum products and chemicals are produced or stored, thereby heightening the potential consequences of a terrorist attack.

Our review is assessing the FBI's responsibilities and capabilities for preventing and responding to maritime terrorist attacks, including attacks

against seaports. In addition, we are examining the extent of the FBI's interagency coordination of seaport security. While the FBI has lead agency responsibilities to prevent and respond to terrorism in the United States, the U.S. Coast Guard is responsible for securing ports, and state and local agencies as well as various industries also have roles in securing the nation's seaports. These shared responsibilities require the FBI to work closely with various partners to help protect U.S. ports from attack. The OIG report will examine how well the FBI's seaport security efforts are working and identify any areas requiring further attention to better protect this vital aspect of the nation's critical infrastructure.

B. Completed OIG Reviews in the FBI

In the past year, the OIG has completed a series of reviews that examined other important FBI programs and operations. The following provides a summary of the findings of several of those reviews.

FBI Foreign Language Translation Program: In July 2005, the OIG issued a follow-up audit that examined the FBI's progress in improving its ability to translate foreign language materials. A previous OIG review in July 2004 analyzed the backlog of unreviewed Foreign Intelligence Surveillance Act (FISA) material, the FBI's progress in hiring qualified linguists to translate critical foreign language materials, the FBI's prioritization of its translation workload, and the FBI's Quality Control Program for linguists.

The July 2004 audit found that the FBI's collection of material requiring translation had outpaced its translation capabilities, and the FBI could not translate all its foreign language counterterrorism and counterintelligence material. The audit also found that the FBI had difficulty in filling its need for additional linguists. In addition, the audit reported that the FBI's digital audio collection systems had limited storage capacity and that untranslated audio sessions were sometimes deleted from the system to make room for new incoming audio sessions. The audit concluded that the FBI was not in full compliance with the standards it had adopted for quality control reviews of the work of newly hired linguists, as well as annual reviews of permanent and contract linguists. The report made 18 recommendations to help the FBI improve its foreign language translation operations, and the FBI generally agreed to implement these changes.

The OIG conducted a follow-up audit, which we issued in July 2005, to evaluate the FBI's progress in responding to the findings and recommendations of the July 2004 report. The follow-up review concluded that the FBI has taken important steps to improve the operations of the foreign language translation program. For example, the FBI now sets specific target staffing levels for linguists that account for attrition. In addition, although we found during our

follow-up review that unreviewed translation materials still were being deleted, no unreviewed counterterrorism or Al Qaeda sessions had been deleted.

However, the follow-up review found that key deficiencies remain in the FBI's foreign language translation program, including a continuing backlog of unreviewed material, some instances where high-priority material has not been reviewed within 24 hours in accordance with FBI policy, and continued challenges in meeting linguist hiring goals. In addition, implementation of the Quality Control Program for linguists has been slow.

With regard to unreviewed material, our follow-up review found that the FBI's collection of audio material continues to outpace its ability to review and translate that material, and the amount of unreviewed FBI counterterrorism and counterintelligence audio material has increased since our July 2004 report. In counterterrorism cases, according to the FBI's data, the backlog of unreviewed audio material has increased from approximately 4,000 hours to approximately 8,000 hours. According to the FBI's calculations, this backlog represents 1.5 percent of total counterterrorism audio collections. The amount of unreviewed counterintelligence material is much larger. While the FBI stated that most of the unreviewed counterintelligence materials may not need to be translated, we found that it has no assurance that all of this material need not be reviewed or translated.

Management of the Trilogy Information Technology Modernization

Project: As noted above, the OIG reviewed the FBI's management of the Trilogy project, which was intended to be the centerpiece of the FBI's efforts to upgrade its information technology infrastructure and replace its antiquated paper-based case management system with a new electronic case management system called the Virtual Case File. Trilogy consisted of three main components: 1) the Information Presentation Component intended to upgrade the FBI's hardware and software; 2) the Transportation Network Component intended to upgrade the FBI's communication networks; and 3) the User Applications Component intended to replace the FBI's most important investigative applications, including the Automated Case Support system, the FBI's current case management system. The first two components of Trilogy provide the infrastructure needed to run the FBI's various user applications, including the planned Virtual Case File.

A February 2005 OIG audit reported that while the FBI had successfully completed the Trilogy infrastructure upgrades, this deployment was completed 22 months later than expected, despite an additional \$78 million provided by Congress after the September 11 terrorist attacks to accelerate deployment of Trilogy's infrastructure components. In addition, the total costs for the infrastructure components of Trilogy increased from \$238.6 million to \$337 million over the course of the project. With regard to the Virtual Case File, the

third phase of Trilogy, the FBI was unable to create and deploy the system after more than 3 years and \$170 million budgeted for the project.

The OIG audit identified a variety of causes for the problems in the Trilogy project, including poorly defined and slowly evolving design requirements for Trilogy, weak information technology investment management practices at the FBI, weaknesses in the way contractors were retained and overseen, the lack of management continuity at the FBI on the Trilogy project, unrealistic scheduling of tasks on Trilogy, and inadequate resolution of issues that warned of problems in Trilogy's development.

The Handling of Intelligence Information Prior to the September 11 Attacks: This OIG report examined what intelligence information the FBI had prior to the September 11 attacks that potentially was related to those attacks. Among other issues, the OIG examined the FBI's handling of the Zacarias Moussaoui case; the FBI's handling of an Electronic Communication written by an FBI agent in Phoenix, Arizona (the Phoenix EC) that raised concerns about efforts by Usama Bin Laden to send students to attend United States civil aviation schools to conduct terrorist activities; and intelligence information available to the FBI regarding two of the September 11 hijackers – Nawaf al Hazmi and Khalid al Mihdhar.

In July 2004, the OIG completed and issued its full report, classified at the Top Secret/SCI level, to the Department, the FBI, Congress, the Central Intelligence Agency (CIA), the National Security Agency, and the National Commission on Terrorist Attacks Upon the United States (9/11 Commission). In its final report, the 9/11 Commission referenced the findings from the OIG's report.

After the OIG issued the classified version of our report, several members of Congress asked the OIG to create and release publicly an unclassified version because of the significant public interest in these matters. The OIG therefore created a 371-page unclassified version of the report. However, because the Moussaoui case is still pending before the United States District Court for the Eastern District of Virginia, the rules of that Court prevented the OIG from releasing the unclassified report without the permission of the District Court. The District Court denied the OIG's motion to release publicly the full unclassified version of the report in late April 2005. The OIG therefore redacted from the unclassified report the information requested by Moussaoui's defense counsel that related to Moussaoui and other matters. The Court subsequently granted the OIG's motion to release the redacted report, and the OIG publicly released it on June 7, 2005.

The OIG's report describes the systemic impediments that hindered the sharing of information between the FBI and the CIA, and the report assesses

the individual performance of FBI employees. The report also contains the OIG's recommendations and conclusions relating to the FBI's analytical program, the FISA process, the FBI's interactions with other members of the Intelligence Community, and other matters involved in this review.

In sum, the OIG review found significant deficiencies in the FBI's handling of intelligence information related to the September 11 attacks. Our review concluded that the FBI failed to fully evaluate, investigate, exploit, and disseminate information related to the Phoenix EC and the Hazmi and Mihdhar matter. The causes for these failures were widespread and varied, ranging from poor individual performance to more substantial systemic deficiencies that undermined the FBI's efforts to detect and prevent terrorism.

In its response to the OIG's report, the FBI described changes it has made related to these issues since the September 11 attacks. In addition, the FBI has created a panel to assess whether any action should be taken with regard to the performance of FBI employees described in the OIG report.

Terrorist Screening Center: The OIG recently completed two reviews examining various aspects of the Terrorist Screening Center (TSC), a multi-agency effort to consolidate the federal government's terrorist watch lists and provide 24-hour, 7-day-a-week responses for screening individuals against the consolidated watch list. Prior to establishment of the TSC, the federal government relied on multiple separate watch lists maintained by a variety of agencies to search for terrorist-related information about individuals who, among other things, apply for a visa, attempt to enter the United States through a port of entry, travel internationally on a commercial airline, or are stopped by a local law enforcement officer for a traffic violation.

In an audit undertaken at this Subcommittee's request and completed last month, the OIG examined the TSC's preparations to support the Secure Flight Program, currently under development in the Transportation Security Agency (TSA). The Secure Flight Program is an initiative in which the TSA will compare names of commercial airline passengers to the TSC's consolidated terrorist watch list.

The OIG audit concluded that the TSC has made significant progress in planning and preparing for the September 2005 anticipated launch of the Secure Flight program. The OIG found that the TSC has designed its necessary electronic connections to accommodate the transfer of terrorist watch list records, airline passenger information, and screening results; developed new processes to facilitate law enforcement responses to encounters with individuals who are a match against the consolidated terrorist watch list; and is on schedule for testing its newly established systems and procedures relating to Secure Flight.

However, our review found that the TSA has delayed the implementation date for Secure Flight, first from April 2005 to August 2005, and later to the most recent target date of September 2005. In addition, the TSA has changed its Secure Flight implementation plan and as of July 31, 2005, was unsure how many airlines will participate in the initial phase. As a result, neither the TSC nor TSA knew how many passenger records will be screened and could not project the number of watch list hits that will be forwarded to the TSC for action. This affected the TSC's ability to plan adequately for its role in the Secure Flight program.

The OIG review also indicated that the Secure Flight program has the potential to significantly impact TSC's space, staffing, and funding needs and has resulted in the postponement of several other TSC projects. However, we found that the TSC lacks the ability to adequately estimate the incremental cost of adding programs that increase its range of operations, such as Secure Flight. According to TSC officials, implementing the Secure Flight program requires substantial, cross-cutting modifications and enhancements to the TSC's infrastructure.

Further, TSC officials said they could not easily distinguish Secure Flight funding needs from those necessary for other TSC system enhancements unrelated to Secure Flight. At our request, the TSC prepared a breakdown of FY 2005 and FY 2006 Secure Flight costs. Of the TSC's \$64.23 million in appropriated and supplemental resources for FY 2005, the TSC estimated that a total of about \$21.3 million will be related to Secure Flight.

The OIG made five recommendations to the TSC to help it support the Secure Flight program. These include enhancing the organization's budget formulation and execution capabilities and re-examining the Secure Flight resource estimates as soon as the program is implemented and workload figures are established. The TSC agreed with our findings and recommendations and stated that it is planning corrective action in response.

In a separate review completed in June 2005, the OIG conducted a comprehensive review of the FBI's management of the TSC. This review found that the TSC has made significant strides in creating a new organization and a consolidated watch list, which was a significant accomplishment. However, the OIG review also found that the TSC needed to address weaknesses in its consolidated terrorist watch list database, computer systems, as well as staffing, training, and oversight of the call center.

The OIG concluded that the TSC had not ensured that the information in that database is complete and accurate. For example, the OIG found instances where the consolidated database did not contain names that should have been

included on the watch list and inaccurate or inconsistent information related to persons included in the database.

The OIG also found problems with the TSC's management of its information technology, a critical part of the terrorist screening process. From its inception, the TSC's Information Technology Branch – staffed with numerous contractors – did not provide effective leadership over the agency's information technology functions. In addition, the TSC experienced significant difficulty in hiring qualified staff with adequate security clearances to perform information technology functions.

The report offered 40 recommendations to the TSC to address areas such as database improvements, data accuracy and completeness, call center management, and staffing. The TSC generally agreed with the recommendations and in some cases provided evidence that it has taken action to correct the weaknesses that the audit identified.

FBI Efforts to Hire, Train, and Retain Intelligence Analysts: In May 2005, the OIG issued an audit report that examined FBI efforts to hire, train, and retain intelligence analysts. Since the September 11 terrorist attacks, the FBI has attempted to hire, train, and use more fully qualified intelligence analysts. In the 3 years since the attacks, the number of FBI analysts grew from 1,023 analysts in October 2001 to 1,403 analysts in October 2004 – a net increase of 380 intelligence analysts, or 37 percent.

Yet, the OIG report found that while the FBI has made progress in hiring and training intelligence analysts, several areas were in need of improvement. For example, the FBI fell short of its fiscal year (FY) 2004 hiring goal by 478 analysts and ended the fiscal year with a vacancy rate of 32 percent. At the end of FY 2004, the FBI had hired less than 40 percent of its goal of 787 analysts.

The audit found that the analysts that the FBI hired generally were well qualified. But the FBI has made slow progress toward developing a quality training curriculum for new analysts. The initial basic training course offered to analysts from 2002 to 2004 was not well attended and received negative evaluations. As a result, the FBI initiated a revised 7-week training course in September 2004.

FBI analysts who responded to an OIG survey indicated that generally they were satisfied with their work assignments, believed they made a significant contribution to the FBI's mission, and were intellectually challenged. However, newer and more highly qualified analysts were more likely to respond negatively to OIG survey questions on these issues. For example, 27 percent of the analysts hired within the last 5 years reported

dissatisfaction with their work assignments, compared to 13 percent of the analysts hired more than 5 years ago.

Further, the intelligence analysts reported on the survey that work requiring analytical skills accounted for about 50 percent of their time. Many analysts reported performing administrative or other non-analytical tasks, such as escort and phone duty. In addition, some analysts said that not all FBI Special Agents, who often supervise analysts, understand the capabilities and functions of intelligence analysts.

The OIG report made 15 recommendations to help the FBI improve its efforts to hire, train, and retain intelligence analysts, including recommendations that the FBI establish hiring goals for intelligence analysts based on the forecasted need for intelligence analysts and projected attrition; implement a better methodology for determining the number of intelligence analysts required and for allocating the positions among FBI offices; and assess the work done by intelligence analysts to determine what is analytical in nature and what general administrative support of investigations can more effectively be performed by other support or administrative personnel. The FBI agreed with the OIG recommendations.

Department of Justice Counterterrorism Task Forces: In a June 2005 report, the OIG issues a report that examined the operation of DOJ Counterterrorism task forces and whether gaps, duplication, or overlap existed in the task forces' work. Three of the five groups we examined – the Joint Terrorism Task Forces (JTTFs), the National Joint Terrorism Task Force, and the Foreign Terrorist Tracking Task Force – are led by the FBI.

The OIG review concluded that the terrorism task forces generally functioned well, without significant duplication of effort, and that they contributed significantly to the Department's goal of preventing terrorism. However, the OIG review identified a series of management and resource problems affecting the operation of the task forces. These included the need for more stable leadership among the task forces, better training for participants, and additional resources. For example, many JTTF members stated that frequent turnover in leadership of the JTTFs affected the structure and stability of the JTTFs and their terrorism investigations.

In addition, the review found that the urban-based JTTFs do not consistently coordinate their activities to share information with the law enforcement agencies and first responders in rural and remote areas within their jurisdictions. We also found that the FBI has not signed Memorandums of Understanding defining the roles, responsibilities, and information-sharing protocols with all of the agencies participating on the task forces. The OIG report provided 28 recommendations to help the FBI and the Department

improve the operations of its various counterterrorism task forces. The FBI generally agreed with the recommendations and agreed to take corrective action.

Follow-up Review of the Status of IDENT/IAFIS Integration: In December 2004, the OIG completed a report that examined efforts to integrate the federal government's law enforcement and immigration agencies' automated fingerprint identification databases. Fully integrating the automated fingerprint system operated by the FBI (IAFIS) and the system operated by the Department of Homeland Security (IDENT) would allow law enforcement and immigration officers to more easily identify known criminals and known or suspected terrorists trying to enter the United States, as well as identify those already in the United States. The December 2004 report was the fifth OIG report in 4 years that monitors the progress of efforts to integrate IAFIS and IDENT.

The December 2004 OIG report found that the congressional directive to fully integrate the federal government's various fingerprint identification systems has not been accomplished because of high-level policy disagreements among the Departments of Justice, Homeland Security, and State regarding such integration. The key policy disagreement was a dispute over how many fingerprints should be taken from foreign visitors to the United States for enrollment into the Department of Homeland Security's (DHS) US-VISIT system.

Our December 2004 report made six recommendations to the Department of Justice, four of which were directed to the FBI. The report again recommended that the Departments of Justice and Homeland Security enter into a Memorandum of Understanding to guide the integration of IAFIS and IDENT.

The FBI has been addressing our recommendations, including the recommendation to increase its transmission of fingerprints of known or suspected terrorists to the DHS from monthly to weekly and identifying the costs and capacity needed to upgrade IAFIS. In April 2005, we learned that the federal government's Homeland Security Committee had adopted a uniform federal biometric standard of ten fingerprints for enrollment. Accordingly, in July 2005, in connection with a restructuring of the DHS, the DHS announced that it would require US-VISIT – which currently takes two fingerprints for enrollment and identify verification – to begin taking ten fingerprints from visitors upon initial entry into the United States, with continued use of two-fingerprint verification for subsequent entry. We believe these steps address our recommendation and should facilitate the development of interoperable automated fingerprint identification systems.

DNA Reviews: In 2004, the OIG completed two reviews examining various aspects of DNA issues. In the first review, completed in May 2004, the OIG examined vulnerabilities in the protocols and practices in the FBI's DNA Laboratory. This review was initiated after it was discovered that an examiner in a DNA Analysis Unit failed to perform negative contamination tests, and the Laboratory's protocols had not detected these omissions. The OIG's review found that certain of the FBI Laboratory's DNA protocols were vulnerable to undetected, inadvertent, or willful non-compliance by DNA staff, and the OIG report made 35 recommendations to address these vulnerabilities. The FBI agreed to amend its protocols to address these recommendations and to improve its DNA training program.

In a second review, the OIG audited laboratories that participate in the FBI's Combined DNA Index System (CODIS), a national database maintained by the FBI that allows law enforcement agencies to search and exchange DNA information. The OIG's CODIS audits identified concerns with some participants' compliance with quality assurance standards and with their uploading of unallowable and inaccurate DNA profiles to the national level of CODIS.

IV. CONCLUSION

In conclusion, I believe the FBI has made progress in addressing its changed priorities since the September 11 terrorist attacks. But significant challenges and deficiencies remain, as various OIG reports have found. The FBI needs more improvement in critical areas such as upgrading its information technology systems; hiring, training, and using intelligence analysts; timely and accurately reviewing and translating foreign language material; sharing information effectively within and outside the FBI; ensuring compliance with Attorney General Investigative Guidelines; and promoting continuity of personnel in key positions. While I believe that Director Mueller is leading the FBI in the right direction, the FBI needs to make significant improvements as it continues this transformation. To assist in this effort, the OIG will continue to monitor the FBI's progress and conduct reviews in important FBI programs.